IT Security Procedural Guide: Lightweight Security Authorization Process CIO-IT Security-14-68

June 13, 2014

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change

Approval

IT Security Procedural Guide: Lightweight Security Authorization Process CIO-IT Security-14-68 is hereby approved for distribution.

X

Kurt D. Garbars
Chief Information Security Officer

Table of Contents

Introduction

The General Services Administration (GSA) Lightweight Security Authorization Process is specific to new GSA information systems pursuing an agile development methodology AND residing on infrastructures that have a GSA Authorization to Operate (ATO) concurred by the GSA Chief Information Security Officer (CISO) or a FedRAMP ATO. Such systems at the FIPS 199 Moderate impact level may pursue a limited ATO for the pilot period of the project, not to exceed one year. The limited ATO will be based on the Lightweight Security Assessment and Authorization (A&A) process defined in this guide. The period of the limited ATO is used to conduct full security assessment and authorization consistent with requirements in GSA IT Security Procedural Guide 06-30, *Managing Enterprise Risk,* resulting in a new three-year ATO. FIPS 199 Low impact information systems in the Office of the Chief Information Officer (GSAIT) organization operating in such environments may utilize the process herein to achieve a full three-year authorization.

The Lightweight A&A process leverages to the greatest extent possible, the inherent flexibility in the application of security controls noted in Special Publication 800-53 Revision 4 to more closely align with business requirements (i.e., DevOps and agile development) and the environments of operation (i.e., environments that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO). The process is focused on operational security from both a functional and assurance perspective and not on adherence to static checklists or the generating of large volumes of security authorization paperwork. Currently, the process supports systems that use Amazon Web Services (AWS), but will be expanded to cover other cloud service provider environments.

This guide describes key activities in the Lightweight ATO process including system security authorization and continuous monitoring. The steps in the process are outlined below.

- RMF Step 1 - Categorize Information System
- RMF Step 2 – Select Security Controls
- RMF Step 3 – Implement Security Controls
- RMF Step 4 – Assess Security Controls
- RMF Step 5 – Authorize Information System
- RMF Step 6 – Monitor Security Controls

1.1 Purpose

This IT Security Procedural Guide: *Lightweight Security Authorization Process* defines the A&A process for a limited ATO for FIPS 199 Moderate applications; and, full three-year authorizations of FIPS 199 Low impact applications in the GSAIT organization pursuing an agile development methodology AND residing on infrastructures that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO.

1.2 Policy

GSA Instructional Letter (CIO-IL-14-02), dated March 10, 2014, states:

2 Lightweight Security Authorization Process

2.1 RMF Step 1 – Categorize Information System

The first step in the process is to determine the FIPS 199 security categorization level of the information system. The Lightweight ATO process is applicable to FIPS 199 Low and Moderate systems only. FIPS 199 Moderate systems may achieve a 1-year limited authorization while FIPS 199 Low impact information systems in the GSAIT organization may utilize the process to achieve a full three-year security authorization. The following tasks detail the actions in RMF Step 1.

TASK 1-1: Security Categorization - Categorize the information system and document the results of the security categorization in the System Security Plan (SSP); utilize the SSP template provided in Appendix B of this guide. The security categorization process is carried out by the System/Data Owner in cooperation and collaboration with appropriate organizational officials with information security/risk management responsibilities including but not limited to the AO, ISSM, and ISSO. The process for determining the appropriate impact level is outlined in *FIPS 199, Standard for Security Categorization of Federal Information and Information Systems* and the companion guide *NIST SP 800-60*, *Guide for* Mapping *Types of Information and Information Systems to Security Categories.* Please refer to these documents to categorize the information system.

TASK 1-2: Information System Description - Describe the information system (including system boundary) and document the description in the SSP. The SSP provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. Descriptive information about the information system is documented in sections 1-12 of the security plan. The level of detail provided in the security plan should be commensurate with the security categorization of the information system. The following sections should be sufficiently detailed:

- Section 2 of the SSP must describe the FIPS 199 categorization of the system. It must be supported by an FIPS 199/NIST 800-60 analysis.
- Section 9 of the SSP must describe the function or purpose of the system and the information processes.
- Section 10 of the SSP must provide a description of the technical system including an inventory of all hardware, software, and networking devices in the authorization boundary. The inventory shall be presented in table format and identify hardware, software, and communications equipment with host name, IP address, and hardware, operating system, and application version information.

- Section 11 of the SSP must list all interconnections including the system name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, authorization to operate status, and the name of the authorizing official. Per GSA IT Security Policy 2100.1*, "Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the Authorizing Officials of both systems prior to connecting a system not under a single Authorizing Official's control in accordance with NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems." Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc."*

TASK 1-3: Information System Registration - Register the information system with the appropriate organizational program/management offices and the Office of the Chief Information Security Officer (OCISO). The ISSO shall add the system to the Lightweight Security Authorization Process ATO Tracking Sheet available on Google Docs at:

https://docs.google.com/a/gsa.gov/spreadsheets/d/1ZtFqu_zr5mr1pNPRpmGoL8lUQ4oEbLqw8HzGdDS_zXA

Further the ISSO shall initiate the Lightweight Security Authorization Process ATO Project Plan available in Appendix A of this guide. The project plan documents the planning and assessment related activities with related milestones, responsibilities and scheduled completion dates.

2.2 RMF Step 2 – Select Security Controls

TASK 2-1: Security Control Selection - The key security controls required for the Limited ATO Process are identified below.

NIT 800-53 R4 Control ID	Control Title	Applicability	
		FIPS-199 Low Impact	FIPS-199 Moderate Impact
AC-2	Account Management	**X**	**X**
AU-2	Audit Events	**X**	**X**

AU-6	Audit Review, Analysis, and Reporting	**X**	**X**
CA-8	Penetration Testing	**X**	**X**
CM-2	Baseline Configuration	**X**	**X**
CM-3	Configuration Change Control	**X**	**X**
CM-6	Configuration Settings	**X**	**X**
CM-8	Information System Component Inventory	**X**	**X**
IA-2	Identification and Authentication (Organizational Users)	**X**	**X**
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	**X**	**X**
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	**X**	**X**
IA-2 (12)	Identification and Authentication | Acceptance of PIV Credentials * Consult with OCISO for Applicability	**X**	**X**
PL-8	Information Security Architecture	**X**	**X**
RA-5	Vulnerability Scanning	**X**	**X**
SA-22	Unsupported System Components	**X**	**X**
SA-11 (1)	Developer Security Testing and Evaluation| Static Code Analysis	**X**	**X**
SC-7	Boundary Protection	**X**	**X**
SC-13	Cryptographic Protection | FIPS Validated Cryptography	**X**	**X**
SC-28 (1)	Protection of Information At Rest | Cryptographic Protection * Applicable to systems with Personally Identifiable Information Only		**X**
SI-2	Flaw Remediation	**X**	**X**
SI-4	Information System Monitoring	**X**	**X**
SI-10	Information Input Validation	**X**	**X**

The key controls required are applicable to FIPS 199 Low- and Moderate- impact as defined in the above table for systems pursuing an agile development methodology and residing on infrastructures that have a GSA ATO concurred by the OCISO or a FedRAMP ATO. The tailored baseline, as necessary, can be supplemented with additional controls and/or control enhancements to address unique organizational and/or system specific needs based on a risk assessment (either formal or informal) and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances. Additional controls are at the discretion of the CISO and the AO in coordination with the ISSM and ISSO.

Document the selected security controls including any controls or enhancements selected above the baseline for the information system in the SSP using the template provided in Appendix B.

TASK 2-2: Monitoring Strategy - Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation. GSA IT Security Procedural Guide 08-39, *FY 2014 IT Security Program Management Implementation Plan* can be used as the plan. The guide identifies key security milestones and measures of progress for implementation. The plan has been reviewed and signed off by every GSA S/SO AO.

TASK 2-3: Security Plan Approval - Review and approve the security plan. The System Owner shall jointly develop the security plan with the ISSO. The completed SSP shall be submitted to the respective OCISO ISSO support division (i.e., Services ISSO (ISS) or Staff Offices ISSO (IST)) Information System Security Manager (ISSM), Division Director, and to the OCISO Security Engineering (ISE) division to determine if the plan is complete, consistent, and satisfies the security requirements for the information system. ISE will evaluate the security architecture and must approve it; the ISS/IST ISSM and Division Director must approve the SSP.

Based on the results of the review, the SSP may require further update or may be approved. The authorizing official or designated representative, by approving the security plan, agrees to the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system; allowing Step 3 of the RMF to begin.

2.3 RMF Step 3 – Implement Key Security Controls and AWS Customer Responsibilities

TASK 3-1: Security Control Implementation – Implement the key security controls in Task 2-1 and the AWS Customer Responsibilities defined in Appendix C of this guide. The AWS EC2 Customer Responsibility Matrix identifies the customer control considerations that are customer responsibilities. The customer responsibilities are presented in checklist format and must be reviewed and implemented by the Program Office/ System Owner. The system owner

shall attest to implementation of the Cloud Service Provider determined customer responsibilities.

Security tools shall be coordinated with the OCISO Security Operations (ISO) division and as much as possible integrate with what is currently used at GSA OR what GSA OCISO proposes to use, particularly in cloud environments such as Amazon Web Services. IT systems shall be configured and hardened using GSA IT security hardening guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the Authorizing Official and concurred by the OCISO. Implemented hardening checklists must be integrated with Security Content Automation Protocol (SCAP) content if available and/or to the greatest extent possible.

TASK 3-2: Security Control Documentation - Document the security control implementation in the SSP using the template provided in Appendix B. Security controls are documented in section 13 of the SSP. This section must provide a thorough description of how each of the required controls are implemented or planned to be implemented. The SSP should also address platform dependencies and include any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail sufficient to support control assessment in RFM Step 4.

2.4 RMF Step 4 – Assess Security Controls

TASK 4-1: Security Control Assessment - Upon implementation of security controls in RMF Step 3, security control assessment will be performed by the OCISO ISSO Division(s) (ISS/IST) to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.

Assessment activities begin upon instantiation (i.e., build out) of the cloud environment and supported application, hardening consistent with the Lightweight Security Authorization Process control requirements, code freeze, a fully developed and approved system security plan, and provision of authentication information to the AWS environment, virtual machines, and hosted application. The assessment activities will begin with a formal kick-off meeting including ALL stakeholders to review and finalize the Security Assessment Project Plan (see Appendix A).

An Integrated Project Team (IPT) approach inclusive of the team responsible for the infrastructure, application developers, system owner, OCISO, and other stakeholders (as necessary) is required to complete assessment activities in a timely fashion (i.e., normally six (6) weeks. The expected ATO timeline could be delayed without full commitment from all parties to fully develop the environment/application consistent with the minimum requirements identified in this guide, provide requisite access to the environment, servers, and applications, and/or timely remediation of deficiencies identified during assessment.

The table below identifies the key controls requiring assessment, the test method used, and the responsible assessor.

NIST 800-53 R4 Control ID	Control Title	Applicability		Type of Testing	Assessment Responsibility
		FIPS- 199 Low Impact	FIPS- 199 Moderate Impact		
AC2	Account Management	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console (IAM)	ISSO Division (ISS or IST)
AU2	Audit Events	**X**	**X**	• Configuration Scan • 53A Controls Assessment • SSP Review	ISSO Division (ISS or IST)
AU6	Audit Review, Analysis, and Reporting	**X**	**X**	• 53A Controls Assessment • SSP Review	ISSO Division (ISS or IST)
CA-8	Penetration Testing	**X**	**X**	• Grey Box Penetration Testing (multiple tools)	Security Engineering Division (ISE)
CM-2	Baseline Configuration	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console (Cloud Formation)	ISSO Division (ISS or IST)
CM-3	Configuration Change Control	**X**	**X**	• 53A Controls Assessment • SSP Review	ISSO Division (ISS or IST)
CM-6	Configuration Settings	**X**	**X**	• Operating System Configuration Scanning • Database Configuration Scanning • 53A Controls Assessment • SSP Review	ISSO Division (ISS or IST) – Controls Assessment Program Office/ SecOps Division (ISO) * - Vulnerability Scanning *ISO will perform Configuration Scanning, where possible. For environments not supported by OCISO, the infrastructure/application

					development team will be responsible for instantiating a scanning solution and the performance of necessary configuration scans.
CM-8	Information System Component Inventory	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console (IAM)	ISSO Division (ISS or IST)
IA-2	Identification and Authentication (Organizational Users)	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console (IAM)	ISSO Division (ISS or IST)
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console (IAM)	ISSO Division (ISS or IST)
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console (IAM)	ISSO Division (ISS or IST)
IA-2 (12)	Identification and Authentication | Acceptance of PIV Credentials * Consult with OCISO for Applicability	**X**	**X**	• 53A Controls Assessment • SSP Review	ISSO Division (ISS or IST)
PL-8	Information Security Architecture	**X**	**X**	• 53A Controls Assessment • SSP Review • OCISO Security Engineering Review and Approval	ISSO Division (ISS or IST)- Controls Assessment Security Engineering Division (ISE) - ISE performs security architecture review

RA-5	Vulnerability Scanning	**X**	**X**	• 53A Controls Assessment • SSP Review • Operating System Vulnerability Scanning • Web Application Vulnerability Scanning	ISSO Division (ISS or IST) – Controls Assessment Program Office/ SecOps Division (ISO) * - Vulnerability Scanning *ISO will perform Web Application Scanning and operating system vulnerability scanning, where possible. For environments not supported by OCISO, the infrastructure/application development team will be responsible for instantiating a scanning solution and the performance of necessary operating system vulnerability scans.
SA-11 (1)	Developer Security Testing and Evaluation| Static Code Analysis	**X**	**X**	• CheckMarx • Fortify	Security Engineering Division (ISE)
SA-22	Unsupported System Components	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection and review of assessment results from CA-8, CM-6, CM-8, and RA-5	ISSO Division (ISS or IST)
SC-7	Boundary Protection	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console (Virtual Private Cloud (VPC)) • Penetration Testing	ISSO Division (ISS or IST) – Controls Assessment Security Engineering Division (ISE) will perform Penetration Testing to verify boundary controls.
SC-13	Cryptographic Protection	**X**	**X**	• 53A Controls Assessment • SSP Review	ISSO Division (ISS or IST)

				• http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm • https://www.ssllabs.com/ssltest/index.html	
SC-28 (1)	Protection of Information At Rest | Cryptographic Protection * Applicable to system with Personally Identifiable Information Only		**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console	ISSO Division (ISS or IST)
SI-2	Flaw Remediation	**X**	**X**	• Controls Assessment • SSP Review • Vulnerability Assessment • Web Application Vulnerability Assessment • Penetration Testing	ISSO Division (ISS or IST) – Controls Assessment Program Office/ SecOps Division (ISO)* - Vulnerability Scanning *ISO will perform Vulnerability and Web Application Scanning, where possible, to determine flaw remediation. Security Engineering Division (ISE) – ISE performs Penetration Testing to verify flaw remediation.
SI-4	Information System Monitoring	**X**	**X**	• 53A Controls Assessment • SSP Review • Manual Inspection via AWS Console (IAM)	ISSO Division (ISS or IST)
SI-10	Information Input Validation	**X**	**X**	• 53A Controls Assessment • SSP Review • Penetration Testing	ISSO Division (ISS or IST) – Controls Assessment Security Engineering Division (ISE) – ISE will perform Penetration Testing to verify input

					validation.

The sections below define each of the assessment types further.

Key Controls Assessment

The security controls assessment is performed by the ISSO. The security controls assessment of the key NIST 800-53 R4 controls will be carried out using the GSA modified NIST 800-53A assessment test cases provided in Appendix D of this guide. Controls assessment will include documentation review, manual validation/review using the AWS Web Console, and technical controls assessment. Assessment will focus on the key security controls identified in Task 2-1.

CM-6 Configuration Settings - Operating System and Database Security Configuration Analysis

Security configuration analysis is performed by the OCISO SecOps Division and/or the contractor organization supporting the information system (as per contract). For GSA Enterprise Cloud Environments planned to be supported by the OCISO, the OCISO SecOps Division will be able to support configuration scanning; for other environments, the supporting infrastructure/application development team will be responsible for instantiating a vulnerability scanning solution and the performance of necessary configuration scanning.

Configuration scanning is performed as an authenticated scan using a combination of automated scanning tools (e.g., nCircle, Nessus, etc), and manual review. For cloud environments such as AWS, the authenticated scan shall be conducted from within the VPC supporting the information system to allow full access to all server settings and configurations. Configuration scans must align with the related GSA or CIS benchmark used to harden and configure the server(s).

RA-5 Vulnerability Scanning / SI-2 Flaw Remediation

Operating System Vulnerability Scan

Operating system vulnerability scanning is performed by the OCISO SecOps Division and/or the contractor organization supporting the information system (as per contract). For GSA Enterprise Cloud Environments planned to be supported by the OCISO, the OCISO SecOps Division will be able to support vulnerability scanning; for other environments, the supporting infrastructure/application development team will be responsible for instantiating a vulnerability scanning solution and the performance of necessary vulnerability scanning.

Vulnerability scanning will be performed as an authenticated scan using a combination of automated scanning tools (e.g., nCircle, Nessus, etc), and manual review. For cloud environments such as AWS, the authenticated scan shall be conducted from within the VPC to allow full access to all server settings and configurations.

Web Application Vulnerability Scan

Web application vulnerability scanning is performed by the OCISO SecOps Division (ISO) and/or the contractor organization supporting the information system (as per contract). Testing is

performed from external scanning systems against the information system using a variety of automated and manual scanning tools. The main purpose of the Web Application Vulnerability Scan is to discover and enumerate any deficiencies in the exposed web interface that could be leveraged by an attacker to gain access to unauthorized systems or data. Web application scanning focuses on the Open Web Application Security Project (OWASP) Top Ten Most Critical Web Applications Security Vulnerabilities, 2013 Update. ISO utilizes HP WebInspect for web application scanning.

CA-8) Penetration Testing

Penetration Testing is performed by the OCISO Security Engineering Division in agreement with GSA IT Security Procedural Guide 11-51, "*Conducting Penetration Test Exercises*". The Penetration Test is performed as a gray-box test insofar that we know the IP address space, system configuration, and architecture of the target system. Testing activities use primarily manual methodologies.

SA-11 (1) Developer Security Testing and Evaluation | Code Analysis

Static code analysis is performed by the OCISO Security Engineering Division. Static code analysis is performed with CheckMarx and Fortify to determine vulnerabilities in code sets.

TASK 4-2: Security Assessment Report – The security assessment report is prepared by the ISSO documenting the issues, findings, and recommendations from the security control assessment. Document assessment findings w/ recommendation(s) and risk determinations using the template in Appendix E of this guide. The report must individually identify and discuss findings from key controls assessment, ALL Critical, High and Moderate operating system, web application, database, and static code vulnerability scan results, all non-compliant operating system configuration deviations, and all penetration test vulnerabilities.

TASK 4-3: Remedial Action - Conduct initial remediation actions on security controls based on the findings and recommendations of the Security Assessment Report and reassess remediated control(s), as appropriate. Findings that are remediated should be appropriately marked in the SAR. In the SAR, *include ''Mitigated' or 'Resolved' next to the* NIST 800-53 R4 CONTROL HEADING.

2.5 RMF Step 5 – Authorize Information System

Following assessment of the information system in RMF Step 4, the POA&M is updated based on the results of the security assessment and any remedial action to correct findings; the Security Authorization Package is assembled and submitted to the AO for adjudication. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable. The following tasks detail the actions in RMF Step 5.

TASK 5-1: Plan of Action and Milestones – The ISSO prepares the plan of action and milestones based on the findings and recommendations of the Security Assessment Report excluding any

remediation actions taken. The POA&M must include all vulnerabilities (except those identified as *''Mitigated' or 'Resolved'* in the SAR*)* in the information system documented in SAR. The POA&M describes how the System Owner intends to address those vulnerabilities (i.e., reduce, eliminate, or accept vulnerabilities). Use the POA&M template available in Appendix F of this guide.

Update the SSP to reflect the results of the security assessment and any modifications to the security controls in the information system. The SSP should reflect the actual state of the security controls implemented in the system following completion of security assessment activities. This is necessary to account for any modifications made to address recommendations for corrective actions from the security assessor.

Note: For every Open or Outstanding finding in the security assessment report, there must be a related planned action in the POA&M and in the System Security Plan for that 800-53 R4 control or enhancement.

TASK 5-2: Security Authorization Package – The ISSO assembles the Security Authorization Package and submits to the OCISO Policy and Compliance Division (ISP). The security authorization package documents the results of the security assessment. The security authorization package includes:

- System Security Plan
- Security Assessment Report
- Plan of Action and Milestones
- Customer Responsibility Matrix
- Authorization Recommendation (i.e., Certification) Letter
- Authorization Decision Letter

The OCISO ISP Division will review the package and forward to the CISO for concurrence if the package is completed consistent with the requirements in this guide and are free of Critical or High risk findings.

Upon CISO signature, the package can be submitted to the AO for ATO consideration. The security authorization package provides the authorizing official the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

TASK 5-3: Risk Determination - Upon receipt of the FINAL Lightweight System Security Authorization Package that has been reviewed by the OCISO and signed by the CISO, the AO must assess the information provided by the System Owner as documented in the Security Authorization Package regarding the current security state of the system and the recommendations for addressing any residual risks.

TASK 5-4: Risk Acceptance – The AO shall determine, with advisement from the CISO, if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The explicit acceptance of risk is the responsibility of the AO. The AO must consider many factors, balancing security considerations with mission and operational needs. The authorizing official issues an authorization decision for the information system after reviewing all of the relevant information. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable. Following review of the security authorization package and consultation with the agency CISO, the AO must render a decision to:

- Authorize system operation w/out any restrictions on it operation;
- Authorize system operation w/ restriction on its operation. The POA&M must include detailed corrective actions for deficiencies, or;
- Not authorize the system for operation.

2.6 RMF Step 6 – Security Control Monitoring

Configuration management, system control monitoring, system status reporting, and documentation updates makeup the concept of security control monitoring. These activities are performed continuously throughout the system lifecycle. The key tasks involved in continuous monitoring are identified in GSA IT Security Procedural Guide 08-39, *FY 2014 IT Security Program Management Implementation Plan.* The guide is available on the GSA IT security website.

Appendix A: Lightweight Security Authorization Process ATO Project Plan Template

Instruction:
The Lightweight Security Authorization Process ATO Project Plan documents the planning and assessment related activities with related milestones, responsibilities and scheduled completion dates.

The current FY template may be found at (open in Chrome Browser):
https://drive.google.com/a/gsa.gov/?tab=mo#folders/0B4te3p_nyWaUaEszSW5pSm45U0E

Appendix B: AWS Lightweight Security Authorization Process System Security Plan Template

Instruction:
The AWS SSP template is used to documents the required Lightweight Security Authorization Process control requirements at the FIPS 199 Low and Moderate impact levels.

The current FY template may be found at (open in Chrome Browser):
https://drive.google.com/a/gsa.gov/?tab=mo#folders/0B4te3p_nyWaUaEszSW5pSm45U0E

Appendix C: AWS EC2 Customer Responsibility Matrix

Instruction: The AWS EC2 Customer Responsibility Matrix identifies the customer control considerations that are customer responsibilities. The customer responsibilities are presented in checklist format and must be reviewed and implemented by the System Owner. The system owner shall attest to implementation of the Cloud Service Provider determined customer responsibilities.

The current FY template may be found at (open in Chrome Browser):
https://drive.google.com/a/gsa.gov/?tab=mo#folders/0B4te3p_nyWaUaEszSW5pSm45U0E

Appendix D: GSA NIST 800-53 R4 Security Assessment Test Cases for AWS

Instruction: The security assessment test cases below are for Low- and Moderate-impact systems. They are used in RMF Step 4 – Assess Security Controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.

The current FY template may be found at (open in Chrome Browser):
https://drive.google.com/a/gsa.gov/?tab=mo#folders/0B4te3p_nyWaUaEszSW5pSm45U0E

Appendix E: Security Assessment Report Template

Instruction: This Security Assessment Report template is completed in RMF Step 4 – Assess Security Controls to document findings from the security assessment of NIST 800-53 R4 controls using the GSA 800-53 R4 Assessment Test Cases, vulnerabilities assessment activities (i.e., os, web, and database scanning), penetration testing, and code review.

Note: The Security Assessment Report must identify all findings from the Security Assessment – not just those that remain open. Findings, for which a corrective action has been implemented, should be identified as 'Mitigated' or 'Resolved'.

The current FY template may be found at (open in Chrome Browser):
https://drive.google.com/a/gsa.gov/?tab=mo#folders/0B4te3p_nyWaUaEszSW5pSm45U0E

Appendix F: Plan of Action and Milestones (POA&M) Template

Instruction:
The POA&M is completed to document vulnerabilities in the information system discovered during security control assessment and/or security control monitoring. The POA&M describes how the System Owner intends to address those vulnerabilities (i.e., reduce, eliminate, or accept vulnerabilities). Reference the GSA IT Security Procedural Guide 09-44, *Plan of Action and Milestones* for POA&M reporting instructions.

The current FY template may be found at (open in Chrome Browser):
https://sites.google.com/a/gsa.gov/fisma/home